Coordinated Science Laboratory

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS

ON THE MINIMUM DISTANCE OF BOSE-CHAUDHURI-HOCQUENGHEM CODES

Vincent Lum and R.T. Chien

REPORT R-328 NOVEMBER, 1966

This work was supported in part by the Joint Services Electronics Program (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract DA 28 043 AMC 00073(E); and in part by the NSF GK-690.

ON THE MINIMUM DISTANCE OF BOSE-CHAUDHURI-HOCQUENGHEM CODES†

by

Vincent Lum* and R. T. Chien
Coordinated Science Laboratory
University of Illinois, Urbana, Illinois

ABSTRACT

In this paper the Mattson-Solomon algorithm is generalized in several directions. Based on the generalized algorithm, several classes of Bose-Chandhuri-Hocquenghem codes are given and shown to possess minimum distance of values greater than those given by the Bose-Chaudhuri-Hocquenghem found.

---

*Now at the IBM Watson Research Center, Yorktown Heights, New York.

†This work is supported in part by National Science Foundation Grant NSF GK-690 and in part by the Joint Services Electronics Program (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract DA 28 043 AMC 00073(E).

I. PRELIMINARY REMARKS

It is well-known that error-correcting codes are very useful for improving the reliability of data-communication and data-storage systems. The signals transmitted in systems with coding are structured to possess certain mathematical properties. At the receiving end these properties are used to recover information from the received message by correcting erroneous symbols.

Among the many known classes of error correcting codes the most important one is a class of codes known as BCH (for Bose-Chandhuri-Hocquenghem) codes. The BCH codes form a subclass of the class of codes known as cyclic codes which can be described naturally with the concepts of polynomial algebra [Peterson 1961].

Consider the ring R of polynomials over a finite field GF(q). We may construct a residue class ring A modulo the ideal generated by the polynomial x^n-1. We shall assume in this paper that $(n,p) = 1$ where p is the characteristic of GF(q). It can be easily shown that A is an algebra of dimension n over GF(q). We shall speak of these residue classes as polynomials of degree $< n$ over GF(q). It can also be shown easily that the ideals in A are ideals generated by factors of x^n-1. These ideals are called cyclic codes. If $x^n-1 = g(x)f(x)$ then $g(x)$ is called the generator polynomial of the code and $f(x)$ its recursion polynomial. Let $v(x)$ be a code word then $v(x) = (a_o x^{n-1} + a_1 x^{n-2} + \cdots a_{n-1})$ and $v(x)$ is divisible by $g(x)$. Furthermore if $f(x) = x^k + b_1 x^{k-1} + \cdots + b_k$ then

$$a_{k+1} + b_1 a_{k+i-1} + \cdots + b_k a_i = 0 \quad i = 0,1,2 \cdots . \qquad (1)$$

It can be easily verified that x^n-1 does not have repeated factors as any such factor would not divide x^n-1 with $(n,p) = 1$. [Elspas 1959]. The solution of (1) can now be written as

$$a_j = c_1\beta_1{}^j + c_2\beta_2{}^j + \cdots + c_k\beta_k{}^j \qquad j = 0,1,2,\cdots \qquad (2)$$

with $c_i \epsilon K$ an extension field of GF(q) and $\beta_1, \beta_2, \cdots \beta_k$ roots of f(x). Given a set of values $a_o, a_1, \cdots a_k$ the values of $c_1, c_2, \cdots ,c_k$ are unique. Since the roots of f(x) are n^{th} roots of unity we may express them as powers of a primitive n^{th} root of unity β and (2) becomes

$$a_j = c_1\beta^{e_1 j} + c_2\beta^{e_2 j} + \cdots c_k\beta^{e_k j} .$$

The Mattson-Solomon polynomial $g_a(x)$ can now be defined as [Mattson and Solomon 1961]

$$g_a(x) = c_1x^{e_1} + c_2x^{e_2} + \cdots + c_kx^{e_k} .$$

It is seen that $a_j = g_a(\beta^j) \quad j = 0,1,2, \cdots$.

The Hamming weight of a polynomial is defined as the number of non-zero terms in it. A critical quantity with regard to the error-correcting capability of a code is its minimum weight, defined as the minimum of the Hamming weights of the polynomials in the code, an ideal in A. With the aid of $g_a(x)$ it is seen that the weight of v(x) is equal to n minus the number of roots of $g_a(x)$ which are also n^{th} roots of unity. Thus the problem of evaluating the weights of the code polynomial has been transformed by Mattson and Solomon to the algebraic problem of evaluating the number of roots of $g_a(x)$ which are also n^{th} roots of unity.

Let us now consider a BCH code generated by the polynomial $g(x)$ such that $g(\beta^i) = 0$, $i = m_o, m_o+1, \ldots, m_o + d_o-2$ where β is a primitive root of K; m_o and d_o are positive integers. Let us further arrange the roots of

$$g_a(s) = c_1 x^{e_1} + \ldots + e_k x^{e_k}$$

such that $0 \leq e_1 < e_2 < e_3 \ldots < e_k \leq n-1$. Since $m_o, m_o+1, \ldots,$ $m_o + d_o-2$ are not roots of $f(x)$ we may write

$$e_{m-1} < m_o < m_o + d_o-2 < e_m \leq n$$

and

$$a_i = g_a(\beta^i) = c_1\beta^{ie_1} + \ldots + c_m\beta^{ie_m} + \ldots + c_k\beta^{ie_k}$$

$$= \beta^{ie_m}[c_m + c_{m+1}\beta^{i(e_{m-1} - e_m)} + \ldots + c_{m-1}\beta^{i(e_1 - e_m)}].$$

We define $p_a(x) = c_1 x^{e'_1} + c_2 x^{e'_2} \ldots + c_k x^{e'_k}$ where $e'_i = e_i - e_m \bmod n$. The power of the leading term in $p_a(x)$ is

$$e_{m-1} - e_m = n - (e_m - e_{m-1}) \leq n - (d_o) \leq n - d_o$$

and $a_i = 0$ only if $p_a(\beta^i) = 0$. It then follows that the weight of a is

$$\begin{aligned} wt(a) &\geq n - \text{no. of zeros of } p_a(x) \\ &\geq n - \deg[p_a(x)] \\ &\geq n - (n - d_o) \\ &= d_o \ . \end{aligned}$$

We have just proved that the minimum weight of a BCH code is at least d_o.*

---

*This fact had been independently proved by H. F. Mattson.

II. GENERAL RESULTS

We shall use h as the degree of extension of K over $F = GF(q)$ where K is the smallest field containing F and all the roots of x^n-1.

Let x^n-1 be factored into irreducible factors over $GF(q)[x]$. Let $f_1(x), f_2(x), \cdots, f_r(x)$ be all the irreducible factors with degree h. Let $b_1, b_2, \cdots, b_r$ be the coefficients of the (h-1)-degree term of $f_1(x), f_2(x), \cdots, f_r(x)$ respectively. We shall concern ourselves with codes whose recursion polynomials f(x) are given in the form of

$$f(x) = (x-1)\varphi_1(x)\varphi_2(x)\cdots\varphi_\delta(x)$$

where each factor of f(x) is in irreducible form. Suppose $\varphi_\delta(x)$ has degree h and $\varphi_\xi(x)$ has degree $h_\xi < h$ for $\xi = 1, 2, \cdots, \delta-1$. Furthermore we shall assume the roots of $\varphi_\delta(x)$ to be primitive n^{th} roots of unity.

We define

$$\begin{aligned} g_a(x) &= c_o + c_{11}x^{e_{11}} + c_{12}x^{e_{12}} + \cdots + c_{1h_1}x^{e_{1h_1}} \\ &\quad + c_{21}x^{e_{21}} + \cdots + c_{2h_2}x^{e_{2h_2}} \\ &\quad + \cdots \\ &\quad + c_{\delta 1}x^{e_{\delta 1}} + \cdots + c_{\delta h}x^{e_{\delta h}} \\ &= c_o + K_1(x) + \cdots + K_{\delta-1}(x) + K_\delta(x) \end{aligned}$$

and

$$p_a(x) = c_o x^{e_o'} + c_{11}x^{e_{11}'} + \cdots + c_{1h_1}x^{e_{1h_1}'}$$

$$+ c_{21}x^{e_{21}'} + \cdots + c_{2h_2}x^{e_{2h_2}'}$$

$$+ \cdots$$

$$+ c_{\delta 1}x^{e_{\delta 1}'} + \cdots + c_{\delta h}x^{e_{\delta h}'}$$

$$= c_o x^{e_o'} + k_1'(x) + \cdots + k_{\delta-1}'(x) + k_\delta'(x) \;.$$

It follows that $(n,e_{\delta k}) = 1$, $1 \leq k \leq h$.

Let us now consider the codes whose recursion polynomial satisfies one of the following two conditions:

(1) $c_{\delta k}$ is the leading coefficient of $p_a(x)$ and $c_{\delta k}^{q^{i_o}}$ is the constant term. Also $(i_o,h) = 1$, and $(n,q^{i_o}-1) = 1$.

(2) c_o is the leading coefficient of $p_a(x)$ and $c_{\delta k}$ is the constant term, or vice versa. $(n,q-1) = 1$.

Let $B_j = c_{\delta 1}\beta^{je_{\delta 1}} + \cdots + c_{\delta h}\beta^{je_{\delta h}}$. Then we have the following theorem.

<u>Theorem 1</u>: Let the code be as defined. Let conditions (1) or (2) be satisfied. If the code has minimum distance equal to d_o, then there exists a field element q_o in a field containing GF(q) such that q_oB_j will take on values $b_1,b_2,\cdots,b_r$ for a set of integers $0 \leq j \leq n-1$.

<u>Proof</u>: Case (1). Condition (1) is met.

Since the minimum distance of the code is d_o, then all the roots of $p_a(x)$ are in U, the set of all n^{th} roots of unity. Thus $c_{\delta k}^{q^{i_o}-1}$ is a product of n^{th} roots of unity, as the set of all n^{th} roots of unity forms a group.

$$(c_{\delta k}^{q^{i_o}-1})^n = 1 \quad \text{or} \quad (c_{\delta k}^{n})^{q^{i_o}-1} = 1$$

By the Reed lemma [Mattson and Solomon 1961], we can write B_j in the form

$$B_j = c_{\delta k}\beta^{je_{\delta k}} + (c_{\delta k}\beta^{je_{\delta k}})^q + \ldots + (c_{\delta k}\beta^{je_{\delta k}})^{q^{h-1}} .$$

Since $c_{\delta k}$ is the leading coefficient, $c_{\delta k} \neq 0$. This implies B_j is not identically zero. $c_{\delta k}^{\,n}$ generates a subgroup G of order R which divides $q^{i_o}-1$. Hence $c_{\delta k}^{\,n} \in GF(q^{i_o})$. As $(q^{i_o}-1,n) = 1$, $(R,n) = 1$ every element in G therefore has a unique n^{th} root. Let $q_1 c_{\delta k}^{\,n} = 1$, q_1 is in G and there exists q_o in G such that $q_o^{\,n} = q_1$. Thus we have $(q_o c_{\delta k})^n = 1$, and so $q_o c_{\delta k}$ is a n^{th} root of unity. Hence $q_o c_{\delta k}\beta^{je_{\delta k}}$ is a n^{th} root of unity for any j. Now

$$q_o B = q_o c_{\delta k}\beta^{je_{\delta k}} + q_o(c_{\delta k}\beta^{je_{\delta k}})^q + \ldots + q_o(c_{\delta k}\beta^{je_{\delta k}})^{q^{h-1}} , \quad (3.1)$$

and $c_{\delta k}^{\,n} \in GF(q^{i_o})$ and $GF(q^h)$. But $(i_o,h) = 1$. Therefore $c_{\delta k}^{\,n} \in GF(q)$ and so does q_o. Then

$$q_o\beta = q_o c_{\delta k}\beta^{je_{\delta k}} + (q_o c_{\delta k}\beta^{je_{\delta k}})^q + \ldots + q_o(c_{\delta k}\beta^{je_{\delta k}})^{q^{h-1}} .$$

$\beta^{je_{\delta k}}$ generates all the n^{th} roots of unity as j takes on all values from 0 to n-1. This implies $q_o c_{\delta k}\beta^{je_{\delta k}}$ will generate all n^{th} roots of unity when j takes all values from 0 to n-1. Since $(i_o,h) = 1$ a subset of these values of j will therefore make the expression $q_o B_j$ equal to the values of $b_1, b_2, \ldots, b_r$ when $q_o c_{\delta k}\beta^{je_{\delta k}}$ becomes a root of $f_i(x)$, $1 \leq i \leq r$. There are $r \cdot h$ values of $0 \leq j \leq n-1$ that would achieve this result.

Case (2). Condition (2) is satisfied.

The leading coefficient of $p_a(x)$ being c_o and constant term being $c_{\delta k}$ or vice versa imply that $\left(\frac{c_{\delta k}}{c_o}\right)^n = 1$, or $c_{\delta k}{}^n = c_o{}^n$. Hence $c_{\delta k}{}^n$ is in GF(q). We can by condition (2) find elements q_o and q_1 in GF(q) such that $q_1 = q_o{}^n$ and $q_1 c_{\delta k}{}^n = (q_o c_{\delta k})^n = 1$. Then

$$q_o B = q_o c_{\delta k}\beta^{je_{\delta k}} + q_o(c_{\delta k}\beta^{je_{\delta k}})^q + \ldots + q_o(c_{\delta k}\beta^{je_{\delta k}})^{q^{h-1}}$$

$$= q_o c_{\delta k}\beta^{je_{\delta k}} + (q_o c_{\delta k}\beta^{je_{\delta k}})^q + \ldots + (q_o c_{\delta k}\beta^{je_{\delta k}})^{q^{h-1}} .$$

The remaining reasoning is the same as in case (1). Q.E.D.

Let $J = \{j_{11}, j_{12}, \ldots, j_{1h}; j_{21}, j_{22}, \ldots, j_{2h}; \ldots; j_{r1}, \ldots, j_{rh}\}$ be the subset of $\{j \mid 0 \leq j \leq n-1\}$ such that $q_o B$ will take on values of $b_1, b_2, \ldots, b_r$, where q_o is as defined in the proof. Let P be the set of integers with values $b_1, b_2, \ldots, b_r$ each repeating h times. Thus $P = \{b_{11}, b_{12}, \ldots, b_{1h}; b_{21}, \ldots, b_{2h}; \ldots; b_{r1}, \ldots, b_{rh}\}$ with $b_{11} = b_{12} = \ldots = b_{1h}$, $b_{21} = b_{22} = \ldots = b_{2h}, \ldots, b_{r1} = b_{r2} = \ldots = b_{rh}$.

With the above hypothesis we know that $q_o B_j$ will take on all the values in P when j takes all values of J. Thus each of $b_{is} \in P$ is associated with exactly one value $j \in J$ which we assume already so arranged that $j = j_{is}$. By association we mean that if $f_i(\beta^{j_{is} e_{\delta k}}) = 0$ and $B^{j_{is} e_{\delta k}} + (\beta^{j_{is} e_{\delta k}})^q + \cdots + (\beta^{j_{is} e_{\delta k}})^{q^{h-1}} = b_{is}$, then b_{is} is associated with j_{is}. Let us now define partitions on the set P as follows.

<u>Definition 1</u>: A partition T_1 divides P into equivalent classes such that $b_{i_1 s_1}$ and $b_{i_2 s_2}$ are in the same class if $j_{i_1 s_1} e_{\xi 1} = j_{i_2 s_2} e_{\xi 1} \bmod n$ for $1 \leq \xi \leq \delta-1$, and $f_{i_1}(\beta^{j_{i_1 s_1} e_{\delta k}}) = 0$, $f_{i_2}(\beta^{j_{i_2 s_2} e_{\delta k}}) = 0$, $1 \leq i_1, i_2 \leq r$ where $b_{i_1 s_1}$ and $b_{i_2 s_2}$ are coefficients of the (h-1)-degree term of $f_{i_1}(x)$ and $f_{i_2}(x)$ respectively.

<u>Theorem 2</u>: In the partitioning as defined above $b_{i_1 s_1}$ and $b_{i_2 s_2}$ will be in the same equivalence class if $K_{\xi j'_{i_1 s_1}} = K_{\xi j'_{i_2 s_2}}$ for $1 \leq \xi \leq \delta-1$ and $q_o B_j(j'_{i_1 s_1}) = b_{i_1 s_1}$ $q_o B_j(j'_{i_2 s_2}) = b_{i_2 s_2}$, i.e. $f_{i_1}(q_o e_{\delta k} \beta^{j'_{i_1 s_1} e_{\delta k}}) = 0$ and $f_{i_2}(q_1 c_{\delta k} \beta^{j'_{i_2 s_2} e_{\delta k}}) = 0$ $1 \leq i_1, i_2 \leq r$.

Proof:

$$(j_{i_1s_1}e_{\xi 1} = j_{i_2s_2}e_{\xi 1}) \underset{\text{mod } n}{} \Rightarrow K_{\xi j_{i_1s_1}} = K_{\xi j_{i_2s_2}} \Rightarrow \beta^{j_{i_1s_1}e_{\xi 1}} = \beta^{j_{i_2s_2}e_{\xi 1}} \quad \text{by definition}$$

$$\Rightarrow \beta^{(j_o'+j_{i_1s_1}')e_{\xi 1}} = \beta^{(j_o'+j_{i_2s_2}')e_{\xi 1}}$$

$$\Rightarrow \beta^{j_o'e_{\xi 1}}\,\beta^{j_{i_1s_1}'e_{\xi 1}} = \beta^{j_o'e_{\xi 1}}\,\beta^{j_{i_2s_2}'e_{\xi 1}}$$

$$\Rightarrow \beta^{j_{i_1s_1}'e_{\xi 1}} = \beta^{j_{i_2s_2}'e_{\xi 1}}$$

$$\Rightarrow K_{\xi j_{i_1s_1}'} = K_{\xi j_{i_2s_2}'} \qquad \text{Q.E.D.}$$

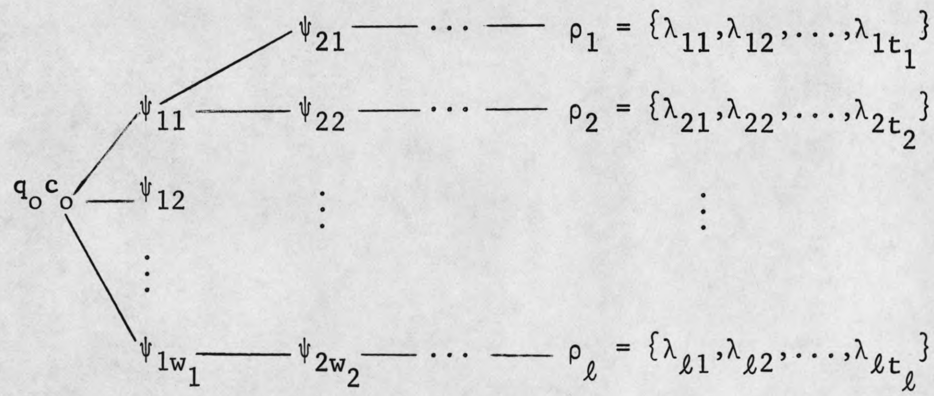
Under the partitioning process of T_1 we have P separated into equivalent classes $\rho_1, \rho_2, \ldots, \rho_\ell$ where ℓ is an integer $\leq r \cdot h$. Let t_k, $1 \leq k \leq \ell$, be the number of elements in each class ρ_k that take on the same value most frequently. Let $\sigma = \sum_{i=1}^{\ell} t_k - v_k$. We are now ready to state the main theorem.

Theorem 3: Let a code be as defined above. Suppose either condition (1) or (2) is satisfied. If $d_o < \sigma$, then the code has minimum distance $\geq d_o+1$.

Proof: The truth of this theorem is obvious if we use a graphical illustration in the form of a tree. We assume the code has minimum distance $= d_o$. Then Theorem 1 and partition T_1 are applicable. Let us consider the number of zero elements of $q_o a_j$ for $0 \leq j \leq n-1$.

$$q_o a_j = q_o c_o + K_{1j} + K_{2j} + \cdots + K_{(\delta-1)j} + q_o B_j \qquad (3.3)$$

Let us concern ourselves with only the values of $j \in J$. Let $K_{\xi j}$, $1 \leq \xi \leq \delta-1$, take w_ξ distinct values as j takes all the values in J, and let these values be $\psi_{\xi 1}, \psi_{\xi 2}, \ldots, \psi_{\xi w_\xi}$. Then we have a graph of the following form.



Of course, the elements $\lambda_{11}, \lambda_{12}, \ldots$ are just elements in the set P.

From this graph it is apparent that each class ρ_k, $1 \leq k \leq \ell$, will contribute at least $t_k - v_k$ nonzero components of $q_o a_j$, $0 \leq j \leq n-1$, when the graph is used in conjunction to Eq. (3.3). Therefore the total number of nonzero components of $q_o a_j$ when j takes all values in J is at least as large as σ. Since $q_o a_j \neq 0$ implies $a_j \neq 0$, there are at least σ nonzero a_j components. But $d_o < \sigma$. This results a contradiction. Therefore the code has minimum distance $\geq d_o + 1$.

Q.E.D.

Note that it is not necessary to show the case that the number of equivalent classes may be smaller than those we have obtained e.g. $K_{\xi 1} = 0$ for some $1 \leq \xi \leq \delta-1$. In this case we actually have a merge of equivalent classes and the contribution of nonzero components to $q_o a_j$ for $j \in J$ can only increase but never decreases.

III. SPECIAL CASES

Case (1): $f(x) = (x-1)(x-\theta)f_{\nu}(x)$, with $\theta \neq 1$,

$\theta \in GF(q)$ and $1 \leq \nu \leq r$.

Let $\theta = \beta^{e_{11}}$. Then we have

$$qe_{11} \equiv e_{11} \quad (n)$$

or

$$(q-1)e_{11} \equiv 0 \quad (n).$$

Partition T_1 in this case actually partitions the set $P' = \{b_1 b_2, \ldots, b_r\}$ into equivalent classes. We can show this by illustrating that b_i, $1 \leq i \leq r$ will always be in the same class regardless of which value of $j \in J$ is associated with b_i.

Let $q_o c_{2k} = \beta^{j_o' e_{2k}}$ and let $\beta^{(j_o'+j_i)e_{2k}}$ be a root of $f_i(x)$, $1 \leq i \leq r$. Then $(\beta^{(j_o'+j_i)e_{2k}})^q$ is also a root of $f_i(x)$ and

$$\beta^{(qj_o'+qj_i)e_{2k}} = \beta^{(j_o'+(q-1)j_o'+qj_i)e_{2k}}$$

$$= q_o c_{2k} \beta^{((q-1)j_o'+qj_i)e_{21}}$$

which states that the integer j corresponding to this second root is $(q-1)j_o' + qj_i = j_i'$. But

$$\beta^{((q-1)j_o'+qj_i)e_{11}} = \beta^{(q-1)j_o' e_{11} + qj_i e_{11}} = \beta^{qj_i e_{11}}$$

since $(q-1)e_{11} \equiv 0 \pmod{n}$. But $\theta = \beta^{e_{11}}$ is an element in the base field GF(q). Thus

$$(\beta^{j_i e_{11}})^q = \beta^{j_i e_{11}} .$$

Hence we have $K_{j_i} = K_{j_i'}$. In other words, two different roots of $f_i(x)$, corresponding to b_{is_1} and b_{is_2}, will always give the same value of $K_j = q_o c_{11}\beta^{je_{11}}$, $0 \leq j \leq n-1$. By Definition 1 they will be in the same equivalent class.

In this special case, then, it is only necessary to calculate one j for each b_i, $1 \leq i \leq r$. This eliminates much of the calculations.

Case (2): $f(x) = (x-1)f_\nu(x)$, $1 \leq \nu \leq r$.

In this particular case we do not even have to apply Definition 1 at all. We have here all b_i, $i = 1,\ldots,r$ belonging to the same class. Thus if n is the number of appearance of a particular value b' which occurs most frequently in the set $\{b_1,b_2,\ldots,b_r\}$, and if we let $\zeta = r-n$, then the only condition we need to look for is whether $d_o < \zeta h$ is satisfied, after either condition (1) or (2) is met.

Case (3): $f(x) = (x-1)f_\nu(x)$, $1 \leq \nu \leq r$ and n a prime integer.

Under the circumstance of n being a prime integer x^n-1 will have factors all of the same degree except for the trivial factor of $x-1$. Hence we have $x^n-1 = (x-1)f_1(x)f_2(x)\ldots f_r(x)$, where each $f_i(x)$, $1 \leq i \leq r$, is irreducible and has degree h. In this case part of the constraints in conditions (1) and (2) are always met, namely the constraints $(n,q^i-1) = 1$ and $(n,q-1) = 1$.

The original result of Mattson-Solomon [1961] is a special case of this case.

Remarks

Theorem 3 shows a particular code may have a minimum distance one bigger than its BCH bound. In certain cases we may apply other results to our conclusion and obtain immediately a minimum distance at least as large as $d_o + 2$. We shall state some of these results.

First let us consider the special case of $q = 2$. In this case if condition (2) in Section II is met, then a minimum distance being equal to an even number implies $c_o = 0$. We can then factor out a power of x from $g_a(x)$ or $p_a(x)$ and check to see if any contradiction results. If the case turns out to be very special and meets Mattson-Solomon [1961] result, we can of course just apply their theorems.

Another result applicable to this end is a theorem given in a report by Mattson [1963]. The theorem is stated as follows.

Theorem 4:

(1) Let $p \equiv 1 \pmod 8$ be prime. Then for each n, $0 \leq 2n < p+1$, in the cyclic $(p, \frac{p+1}{2})$ code over GF(2), either both weights 2n-1 and 2n appear or neither appears.

(2) For $p \equiv -1$ and $3 \mid \frac{p+1}{4}$, then in the cyclic $(p, \frac{p+1}{2})$ code over GF(3), either both weights 3n-1 and 3n appear or neither appears (for $0 < 3n < p+1$).

Also Vera Pless in her paper [1963] mentioned the result of Prange and Gleasaon that may be also useful sometimes. Actually it is only applicable to the original Mattson-Solomon [1961] type of special case.

IV. EXAMPLES

In this section we shall present several different examples. The examples are so chosen that each will illustrate some particular points of the theory presented.

Example 1: Golay (11,6) Code over GF(3)

We all know that the linear Golay (11,6) code has minimum distance equal to 5. The BCH bound for its cyclic version, however, is only 4. We may apply our theory to show that the minimum distance of this cyclic code is 5. The details of this example has appeared elsewhere [Chien and Lum 1966].

Example 2: (73,10) Code over GF(2)

It was found that

$$x^{73} - 1 = (x-1)f_1(x)f_2(x)\dots f_8(x)$$

where $f_i(x)$ for $i = 1,2,\dots,8$ are irreducible over $GF(2)[x]$ and each one is of degree 9. We have here $h = 9$ and $m_o = 1$. The BCH bound for this code is $d_o = 25$. It was found that five coefficients of the 8^{th} degree terms in $f_i(x)$, $i = 1,2,\dots,8$ are 0's and three are 1's. Again we have special case (3) here. ζ as defined in Section III is thus equal to 3. Conditions of Theorem 3 are satisfied and $d_o = 25 < \zeta h = 3.9 = 27$. Thus the code has minimum distance $d \geq 25 + 1 = 26$. But if $d = 26$, then $c_o = 0$. Since for this code, $E(\beta) = \{0,25,50,27,54,35,70,67,61,49\}$, we have

$$g_a(x) = c_o + c_1x^{25} + c_2x^{50} + c_3x^{27} + c_4x^{54} + c_5x^{35} + c_6x^{70} + c_7x^{67} + c_8x^{61} + c_0x^{49} .$$

$c_o = 0$ implies

$$g_a(x) = x^{25}(c_1+c_2x^{25}+c_3x^2+\ldots+c_6x^{45}+\ldots+c_9x^{24}) .$$

The highest degree inside the parenthesis is 45, and therefore $g_a(x)$ can have at most 45 zeros. This means the minimum distance is at least 28, a contradiction to $d = 26$. Hence this code has minimum distance $d \geq 27$.

Example 4: (39,15) Code over GF(2)

The cycles for this code are

$$(1,2,4,8,16,32,25,11,22,5,10,20) \longleftrightarrow f_1(x)$$

$$(3,6,12,24,9,18,36,33,27,15,30,21) \longleftrightarrow f_2(x)$$

$$(7,14,28,17,34,29,19,38,37,35,31,23) \longleftrightarrow f_3(x)$$

$$(13,26) \longleftrightarrow \varphi_1(x)$$

$$(0) \longleftrightarrow (x-1)$$

Let $f(x) = (x-1)\varphi_1(x)\varphi_2(x)$, where $\varphi_2(x) = f_3(x)$, be the recursion polynomial for this code. Then we have $d_o = 7$, $m_o = 1$, $h_1 = 2$, and $h = 12$. Condition (2) is satisfied. We have according to our notation $e_{11} = 13$ and $e_{21} = 7$. We construct the following table for the application of Definition 1. (See Table 2.)

Applying Definition 1 we obtain three equivalent classes. These are

$$\rho_1 = \{b_3, b_3, b_1, b_3, b_3, b_1, b_3, b_3, b_1, b_1, b_1, b_1\}$$

$$\rho_2 = \{b_3, b_3, b_3, b_3, b_1, b_1, b_3, b_1, b_1, b_3, b_1, b_1\}$$

$$\rho_3 = \{b_2, b_2, b_2, b_2, b_2, b_2, b_2, b_2, b_2, b_2, b_2, b_2\}$$

It was found that $b_1 = 0$ and $b_3 = 1$. Thus we have $\sigma = 6 + 6 = 12$ and $d_o = 7 < \sigma = 12$. Hence by Theorem 3, the code has minimum distance $d \geq 8$.

There are numerous codes which the theory in Section III is applicable. Among the simple ones are the (23,12), (43,15), (113,29), (156,16) codes over GF(2), the (11,6), (19,10), (23,12) codes over GF(4) and different others over different finite fields.

Table 1

j	je_{11} mod 39	je_{21} mod 39	Corresponding b_i	j	je_{11} mod 39	je_{21} mod 39	Corresponding b_i
0	0	0	--	20	26	23	b_3
1	13	7	b_3	21	0	30	b_2
2	26	14	b_3	22	13	37	b_3
3	0	21	b_2	23	26	5	b_1
4	13	28	b_3	24	0	12	b_2
5	26	35	b_3	25	13	19	b_3
6	0	3	b_2	26	26	26	--
7	13	10	b_1	27	0	33	b_2
8	26	17	b_3	28	13	1	b_1
9	0	24	b_2	29	26	8	b_1
10	13	31	b_3	30	0	15	b_2
11	26	38	b_3	31	13	22	b_1
12	0	6	b_2	32	26	29	b_3
13	13	13	--	33	0	36	b_2
14	26	20	b_1	34	13	4	b_1
15	0	27	b_2	35	26	11	b_1
16	13	34	b_3	36	0	18	b_2
17	26	2	b_1	37	13	25	b_1
18	0	9	b_2	38	26	32	b_1
19	13	16	b_1				

Examples with $i_o \neq 1$

(i) $n = 113$, $k = 29$ over GF(2)

$h = 28$, $d_o = 17$, $m_o = 33$ (or 65)

(a) Take $m_o = 33$

$$m = 33 + 17 - 1 = 49$$

$$\begin{array}{l} \quad\;\; c_0\ c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7 \\ E(\beta) = \{0, 1, 2, 4, 8, 16, 32, 64, 15, 30, 60, 7, 14, 28, \\ \quad 56, 112, 111, 109, 105, 97, 81, 49, 98, 83, 53, \\ \quad 106, 99, 85, 57\} \end{array}$$

$$\begin{array}{l} E'(\beta) = \{64, 65, 66, 68, 72, 80, 96, 15, 79, 94, 11, 71, \\ \quad 78, 92, 7, 63, 62, 60, 56, 48, 32, 0, 49, 34, 4, \\ \quad 57, 50, 36, 8\}\ . \end{array}$$

Leading coefficient $= c_6 +$ h as degree $= 96$

Constant term $= c_6 q^{15} = c_{21}$

$i_o = 15$, $(i_o, h) = (15, 113) = 1$.

The other condition is satisfied since n = prime. The minimum distance of this code is ≥ 18.

(b) Take $m_o = 65$

$$m = 65 + 17 - 1 = 81$$

$$\begin{array}{l} E(\beta) = \{0, 1, 2, 4, 8, 16, 32, 64, 15, 30, 60, 7, 14, 28, \\ \quad 56, 112, 111, 109, 105, 97, 81, 49, 98, 83, 53, \\ \quad 106, 99, 85, 57\} \end{array}$$

$$E'(\beta) = \{32, 33, 34, 36, 40, 48, 64, 96, 47, 62, 92, 39, 46, 60, 88, 31, 30, 28, 24, 16, 0, 81, 17, 2, 85, 25, 18, 4, 89\} .$$

Leading coefficient $= c_7$

Constant term $= c_7{}^{q^{13}} = c_{20}$

$$i_o = 13 \quad , \quad (13,113) = (i_o,h) = 1.$$

So either choice of m_o will have $i_o \neq 1$.

(ii) $n = 19$, $k = 10$ over GF(4)

(1, 4, 16, 7, 9, 17, 11, 6, 5)

(2, 8, 13, 14, 18, 15, 3, 12, 10)

$h = 9$ $\quad d_o = 5$, $\quad m_o = 4$ (or 12).

(a) $m_o = 4$ $\qquad m = 4 + 5 - 1 = 8$

$$E(\beta) = \{0, 2, 8, 13, 14, 18, 15, 3, 12, 10\}$$

$$E'(\beta) = \{\underset{c_o}{11}, \underset{c_1}{13}, \underset{c_2}{0}, 5, 6, 10, 7, 14, 4, 2\} .$$

Leading coefficient $= c_7$

Constant term $= c_2 = c_7{}^{4^4}$

$$i_o = 4 \qquad (i_o,h) = (4,9) = 1.$$

(b) $m_o = 12$ $m = 12 + 5 - 1 = 16$

$$E(\beta) = \{0, 1, 4, 16, 7, 9, 17, 11, 6, 5\}$$

$$E'(\beta) = \{3, 4, 7, 0, 10, 11, 1, 14, 9, 8\} .$$

Leading coefficient $= c_8$

Constant term $= c_3$

$$C_8^{4^5} = c_3$$

$$i_o = 5, \qquad (i_o, h) = (5,9) = 1.$$

So either choice of m_o will give $i_o \neq 1$. The minimum distance of this code is ≥ 6.

Remarks

A number of additional BCH codes that satisfy the condition states in this paper and therefore possess a minimum distance greater than the BCH bound have been verified by Goethals [1966].

BIBLIOGRAPHY

1. Peterson, W. W., Error-Correcting Codes, MIT Press, 1961.

2. Elspas, B., "The Theory of Autonomous Linear Sequential Networks," IRE Trans., CT-6, 45-60 (1959).

3. Mattson, H. F. and G. Solomon, "A New Treatment of Bose-Chaudhuri Codes," J. SIAM, Vol. 9, No. 4, pp. 654-699, December 1961.

4. Mattson, H. F., "Research Program to Extend the Theory of Weight Distribution and Related Problems for Cyclic Error-Correcting Codes," AFCRL TDR 63-321. Applied Research Laboratory, Sylvania Electronic Laboratory, Waltham, Massachusetts, 1963.

5. Pless, V., "Power Moment Identities on Weight Distribution in Error Correcting Codes," Information and Control, 6, 1963.

6. Chien, R. T. and V. Lum, "On Golay's Perfect Codes and Step-by-Step Decoding," IEEE Transactions on Information Theory, Vol. IT-12, No. 3, pp. 403-404, July, 1966.

7. Goethals, J. M., "Analysis of Weight Distribution in Binary Cyclic Codes," IEEE Trans. on Information Theory, Vol. IT-12, No. 3, p. 401, July, 1966.

Distribution list as of May 1, 1966

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res. & Engrg.
Department of Defense
Washington, D. C. 20301

1 Office of Deputy Director
(Research and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Headquarters
Defense Communications Agency (333)
The Pentagon
Washington, D. C. 20305

20 Defense Documentation Center
Attn: TISIA
Cameron Station, Building 5
Alexandria, Virginia 22314

1 Director
National Security Agency
Attn: Librarian C-332
Fort George G. Meade, Maryland 20755

1 Weapons Systems Evaluation Group
Attn: Col. Finis G. Johnson
Department of Defense
Washington, D. C. 20305

1 National Security Agency
Attn: R4-James Tippet
Office of Research
Fort George G. Meade, Maryland 20755

1 Central Intelligence Agency
Attn: OCR/DD Publications
Washington, D. C. 20505

1 AFRSTE
Hqs. USAF
Room 1D-429, The Pentagon
Washington, D. C. 20330

1 AUL3T-9663
Maxwell Air Force Base, Alabama 36112

1 AFFTC (FTBPP-2)
Technical Library
Edwards AFB, California 93523

1 Space Systems Division
Air Force Systems Command
Los Angeles Air Force Station
Los Angeles, California 90045
Attn: SSSD

1 SSD(SSTRT/Lt. Starbuck)
AFUPO
Los Angeles, California 90045

1 Det. #6, OAR (LOOAR)
Air Force Unit Post Office
Los Angeles, California 90045

1 Systems Engineering Group (RTD)
Technical Information Reference Branch
Attn. SEPIR
Directorate of Engineering Standards
& Technical Information
Wright-Patterson AFB, Ohio 45433

1 ARL (ARIY)
Wright-Patterson AFB, Ohio 45433

1 AFAL (AVT)
Wright-Patterson AFB, Ohio 45433

1 AFAL (AVTE/R. D. Larson)
Wright-Patterson AFB, Ohio 45433

1 Office of Research Analyses
Attn: Technical Library Branch
Holloman AFB, New Mexico 88330

2 Commanding General
Attn: STEWS-WS-VT
White Sands Missile Range
New Mexico 88002

1 RADC (EMLAL-I)
Griffiss AFB, New York 13442
Attn: Documents Library

1 Academy Library (DFSLB)
U. S. Air Force Academy
Colorado 80840

1 FJSRL
USAF Academy, Colorado 80840

1 APGC (PGBPS-12)
Eglin AFB, Florida 32542

1 AFETR Technical Library
(ETV, MU-135)
Patrick AFB, Florida 32925

1 AFETR (ETLLG-I)
STINFO Officer (for Library)
Patrick AFB, Florida 32925

1 AFCRL (CRMXLR)
AFCRL Research Library, Stop 29
L. G. Hanscom Field
Bedford, Massachusetts 01731

2 ESD (ESTI)
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 AEDC (ARO, INC)
Attn: Library/Documents
Arnold AFS, Tennessee 37389

2 European Office of Aerospace Research
Shell Building
47 Rue Cantersteen
Brussels, Belgium

5 Lt. Col. E. P. Gaines, Jr.
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 U. S. Army Research Office
Attn. Physical Sciences Division
3045 Columbia Pike
Arlington, Virginia 22204

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: V. W. Richards
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commandant
U. S. Army Air Defense School
Attn: Missile Sciences Division C&S Dept.
P. O. Box 9390
Fort Bliss, Texas 79916

1 Commanding General
U. S. Army Missile Command
Attn: Technical Library
Redstone Arsenal, Alabama 35809

1 Commanding General
Frankford Arsenal
Attn: SMUFA-L6000 (Dr. Sidney Ross)
Philadelphia, Pennsylvania 19137

1 U. S. Army Munitions Command
Attn: Technical Information Branch
Picatinney Arsenal
Dover, New Jersey 07801

1 Commanding Officer
Harry Diamond Laboratories
Attn: Mr. Berthold Altman
Connecticut Avenue & Van Ness Street N. W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Attn: Technical Director
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army Engineer Geodesy, Intelligence
and Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Attn: Secretary
Fort Leavenworth, Kansas 66270

1 Dr. H. Robl, Deputy Chief Scientist
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
Attn: CRD-AA-IP (Richard O. Ulsh)
Box CM, Duke Station
Durham, North Carolina 27706

1 Superintendent
U. S. Army Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Medical Center
Washington, D. C. 20012

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineer R&D Laboratory
Attn: STINFO Branch
Fort Belvoir, Virginia 22060

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

1 Dr. S. Benedict Levin, Director
Institute for Exploratory Research
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

1 Director
Institute for Exploratory Research
U. S. Army Electronics Command
Attn: Mr. Robert O. Parker, Executive
Secretary, JSTAC (AMSEL-XL-D)
Fort Monmouth, New Jersey 07703

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Attn: AMSEL-SC
RD-D
RD-G
RD-GF
RD-MAF-I
RD-MAT
XL-D
XL-E
XL-C
XL-S
HL-D
HL-L
HL-J
HL-P
HL-O
HL-R
NL-D
NL-A
NL-P
NL-R
NL-S
KL-D
KL-E
KL-S
KL-T
VL-D
WL-D

3 Chief of Naval Research
Department of the Navy
Washington, D. C. 20360
Attn: Code 427

4 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360

3 Chief, Bureau of Weapons
Department of the Navy
Washington, D. C. 20360

2 Commanding Officer
Office of Naval Research Branch Office
Box 39, Navy No. 100 F.P.O.
New York, New York 09510

3 Commanding Officer
Office of Naval Research Branch Office
219 South Dearborn Street
Chicago, Illinois 60604

1 Commanding Officer
Office of Naval Research Branch Office
1030 East Green Street
Pasadena, California

1 Commanding Officer
Office of Naval Research Branch Office
207 West 24th Street
New York, New York 10011

Distribution list as of May 1, 1966 (cont'd.)

1 Commanding Officer
Office of Naval Research Branch Office
495 Summer Street
Boston, Massachusetts 02210

8 Director, Naval Research Laboratory
Technical Information Officer
Washington, D. C.
Attn: Code 2000

1 Commander
Naval Air Development and Material Center
Johnsville, Pennsylvania 18974

2 Librarian
U. S. Naval Electronics Laboratory
San Diego, California 95152

1 Commanding Officer and Director
U. S. Naval Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06840

1 Librarian
U. S. Navy Post Graduate School
Monterey, California

1 Commander
U. S. Naval Air Missile Test Center
Point Magu, California

1 Director
U. S. Naval Observatory
Washington, D. C.

2 Chief of Naval Operations
OP-07
Washington, D. C.

1 Director, U. S. Naval Security Group
Attn: G43
3801 Nebraska Avenue
Washington, D. C.

2 Commanding Officer
Naval Ordnance Laboratory
White Oak, Maryland

1 Commanding Officer
Naval Ordnance Laboratory
Corona, California

1 Commanding Officer
Naval Ordnance Test Station
China Lake, California

1 Commanding Officer
Naval Avionics Facility
Indianapolis, Indiana

1 Commanding Officer
Naval Training Device Center
Orlando, Florida

1 U. S. Naval Weapons Laboratory
Dahlgren, Virginia

1 Weapons Systems Test Division
Naval Air Test Center
Patuxtent River, Maryland
Attn: Library

1 Mr. Charles F. Yost
Special Assistant to the Director of Research
National Aeronautics and Space Administration
Washington, D. C. 20546

1 Dr. H. Harrison, Code RRE
Chief, Electrophysics Branch
National Aeronautics and Space Administration
Washington, D. C. 20546

1 Goddard Space Flight Center
National Aeronautics and Space Administration
Attn: Library, Documents Section Code 252
Greenbelt, Maryland 20771

1 NASA Lewis Research Center
Attn: Library
21000 Brookpark Road
Cleveland, Ohio 44135

1 National Science Foundation
Attn: Dr. John R. Lehmann
Division of Engineering
1800 G Street, N. W.
Washington, D. C. 20550

1 U. S. Atomic Energy Commission
Division of Technical Information Extension
P. O. Box 62
Oak Ridge, Tennessee 37831

1 Los Alamos Scientific Laboratory
Attn: Reports Library
P. O. Box 1663
Los Alamos, New Mexico 87544

2 NASA Scientific & Technical Information Facility
Attn: Acquisitions Branch (S/AK/DL)
P. O. Box 33
College Park, Maryland 20740

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61801

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California

1 Director
Electronics Research Laboratory
University of California
Berkeley 4, California

1 Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

1 Professor A. A. Dougal, Director
Laboratories for Electronics and
Related Sciences Research
University of Texas
Austin, Texas 78712

1 Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

1 Aerospace Corporation
P. O. Box 95085
Los Angeles, California 90045
Attn: Library Acquisitions Group

1 Professor Nicholas George
California Institute of Technology
Pasadena, California

1 Aeronautics Library
Graduate Aeronautical Laboratories
California Institute of Technology
1201 E. California Boulevard
Pasadena, California 91109

1 Director, USAF Project RAND
Via: Air Force Liaison Office
The RAND Corporation
1700 Main Street
Santa Monica, California 90406
Attn: Library

1 The Johns Hopkins University
Applied Physics Laboratory
8621 Georgia Avenue
Silver Spring, Maryland
Attn: Boris W. Kuvshinoff
Document Librarian

1 Hunt Library
Carnegie Institute of Technology
Schenley Park
Pittsburgh, Pennsylvania 15213

1 Dr. Leo Young
Stanford Research Institute
Menlo Park, California

1 Mr. Henry L. Bachmann
Assistant Chief Engineer
Wheeler Laboratories
122 Cuttermill Road
Great Neck, New York

1 University of Liege
Electronic Department
Mathmatics Institute
15, Avenue Des Tilleuls
Val-Benoit, Liege
Belgium

1 School of Engineering Sciences
Arizona State University
Tempe, Arizona

1 University of California at Los Angeles
Department of Engineering
Los Angeles, California

1 California Institute of Technology
Pasadena, California
Attn: Documents Library

1 University of California
Santa Barbara, California
Attn: Library

1 Carnegie Institute of Technology
Electrical Engineering Department
Pittsburgh, Pennsylvania

1 University of Michigan
Electrical Engineering Department
Ann Arbor, Michigan

1 New York University
College of Engineering
New York, New York

1 Syracuse University
Department of Electrical Engineering
Syracuse, New York

1 Yale University
Engineering Department
New Haven, Connecticut

1 Airborne Instruments Laboratory
Deerpark, New York

1 Bendix Pacific Division
11600 Sherman Way
North Hollywood, California

1 General Electric Company
Research Laboratories
Schenectady, New York

1 Lockheed Aircraft Corporation
P. O. Box 504
Sunnyvale, California

1 Raytheon Company
Bedford, Massachusetts
Attn: Librarian

Security Classification

DOCUMENT CONTROL DATA R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) University of Illinois Coordinated Science Laboratory Urbana, Illinois 61801	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

ON THE MINIMUM DISTANCE OF BOSE-CHAUDHURI-HOCQUENGHEM CODES

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (Last name, first name, initial)

Lum, Vincent & Chien, R.T.

6. REPORT DATE	7a TOTAL NO. OF PAGES	7b. NO. OF REFS.
November, 1966	24	7

8a. CONTRACT OR GRANT NO. DA 28 043 AMC 00073(E) b. PROJECT NO. 20014501B31F; Also in part NSF GK-690. c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) R-328 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES

Distribution of this report is unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Joint Services Electronics Program thru U.S. Army Electronics Command Ft. Monmouth, New Jersey, 07703

13. ABSTRACT

In this paper the Mattson-Solomon algorithm is generalized in several directions. Based on the generalized algorithm, several classes of Bose-Chandhuri-Hocquenghem codes are given and shown to possess minimum distance of values greater than those given by the Bose-Chaudhuri-Hocquenghem found.

DD FORM 1 JAN 64 1473

Security Classification

Security Classification

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Error correction						
Reliability						
Digital systems						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization (corporate author) issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers (either by the originator or by the sponsor), also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through ________________."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through ________________."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through ________________."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, roles, and weights is optional.

DD FORM 1473 1 JAN 64

Security Classification